Advantech B+B SmartWorx

Advantech B+B SmartWorx Cryptographic Module

Version 1.0

FIPS 140-2 Non-Proprietary
Security Policy

Level 1 Validation

Document revision 019, February 2016

B+B SmartWorx
Westlink Commercial Park,
Oranmore, Co. Galway, Ireland
http://advantech-bb.com

Prepared for B+B SmartWorx by

Rycombe Consulting Limited
http://www.rycombe.com
+44 1273 476366

Contents

Figures

1 Introduction

This section identifies the cryptographic module; describes the purpose of this document; provides external references for more information; and explains how the document is organized.

1.1 Identification

Module Name	Advantech B+B SmartWorx Cryptographic Module
Module Version	1.0

1.2 Purpose

This is the non-proprietary FIPS 140-2 Security Policy for the Advantech B+B SmartWorx Cryptographic Module, also referred to as “the module” within this document. This Security Policy details the secure operation of Advantech B+B SmartWorx Cryptographic Module as required in Federal Information Processing Standards Publication 140-2 (FIPS 140-2) as published by the National Institute of Standards and Technology (NIST) of the United States Department of Commerce.

1.3 References

For more information on Advantech B+B SmartWorx products please visit: http://advantech-bb.com. For more information on NIST and the Cryptographic Module Validation Program (CMVP), please visit http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.4 Document Organization

This Security Policy document is one part of the FIPS 140-2 Submission Package. This document outlines the functionality provided by the module and gives high-level details on the means by which the module satisfies FIPS 140-2 requirements. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission documentation may be Advantech B+B SmartWorx proprietary or otherwise controlled and releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Advantech B+B SmartWorx.

The various sections of this document map directly onto the sections of the FIPS 140-2 standard and describe how the module satisfies the requirements of that standard.

1.5 Document Terminology

TERM	DESCRIPTION
AES	Advanced Encryption Standard
API	Application Programming Interface
CAVP	Cryptographic Algorithm Validation Program
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program

CSP	Critical Security Parameters
DRBG	Deterministic Random-bit Generator
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
GUI	Graphical User Interface
IKE	Internet Key Exchange
IPC	Inter-process communication
IPsec	Internet Protocol Security, a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session
ISAKMP	Internet Security Association and Key Management Protocol
OpenSSL	An open-source implementation of the SSL and TLS protocols
OS	Operating System
RSA	An algorithm for public-key cryptography. Named after Rivest, Shamir and Adleman who first publicly described it.
SHA	Secure Hash Algorithm
SP	Security Policy
Storage Media	Any media for which Cryptographic Module protection in the form of data encryption is required. Storage Media include internal and external hard drives, memory sticks and floppy disks.
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
XML	Extensible Markup Language

Figure 1 Document terminology

2 Advantech B+B SmartWorx Cryptographic Module

This section provides the details of how the module meets the FIPS 140-2 requirements.

2.1 Overview

The module provides cryptographic services to Advantech B+B SmartWorx products.

2.2 Module Specification

The Advantech B+B SmartWorx Cryptographic Module is a software module that provides cryptographic services to Advantech B+B SmartWorx products.

The module provides a number of FIPS 140 validated cryptographic algorithms for services such as IPsec. The module provides applications with a library interface that enables them to access the various cryptographic algorithm functions supplied by the module.

2.2.1 Hardware, Software and Firmware components

The module is a software module which resides on proprietary hardware (see Figure 3). For the purposes of FIPS 140-2 testing, the module is evaluated running on the Advantech B+B SmartWorx Spectre V3 LTE platform.

The module includes an embedded copy of version 2.0.9 of the OpenSSL FIPS Object Module (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1747).

The module is packaged as a number of distinct binary images:

File Name(s)	Processor	Operating System
pluto, whack, pluto_adns; fipscheck, libfipscheck.so; certutil, modutil, pk12util, libnssdbm3.so, libsoftokn3.so, libfreelbl3.so; libcrypto.so; Kernel	ARM Cortex	Conel Linux 5

Figure 2 Module binary images

2.2.2 Cryptographic Boundary

The cryptographic boundary of the module is the case of the platform on which it is installed. See Figure 3. The module is a software module running on a proprietary hardware platform. The processor of this platform executes all software. All software components of the module are persistently stored within the device and, while executing, are stored in the device local RAM.

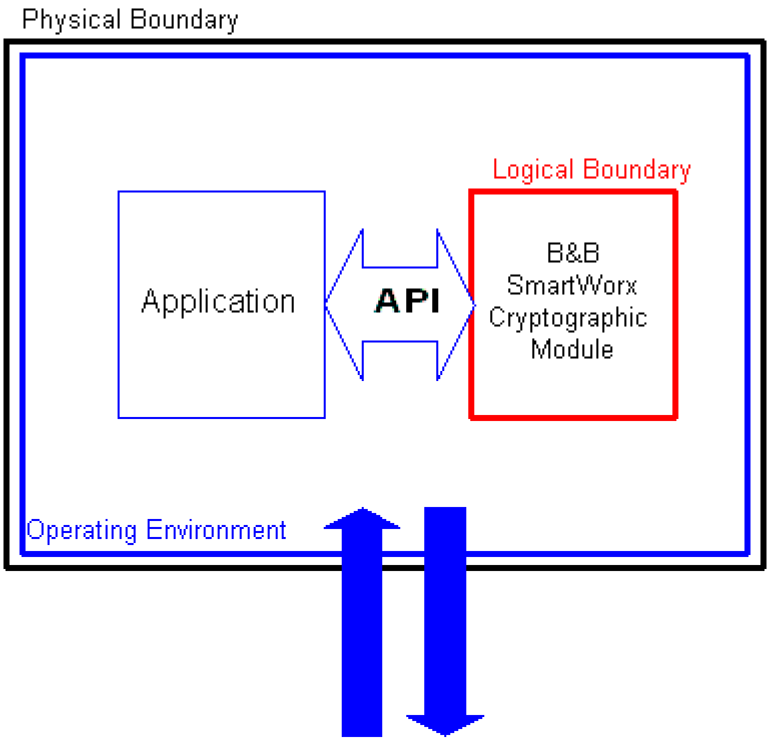

Figure 3 Block Diagram of the Cryptographic Boundary

2.2.3 Scope of Evaluation

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2, with Design Assurance at Level 3.

SECURITY REQUIREMENTS SECTION	LEVEL
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

Figure 4 Security Level specification per individual areas of FIPS 140-2

2.2.4 Cryptographic Algorithms

2.2.4.1 Approved algorithms

The following table provides details of the approved algorithms that are included within the module:

Algorithm type	Algorithm	Status	Notes
Symmetric key	AES	#3515, #3516	AES with 128, 192 or 256 bit keys using ECB, CBC and CTR modes. Used during IKE and ESP.
	Triple DES	#1974, #1975	Three-key Triple DES. ECB and CBC modes. Used during IKE and ESP
Asymmetric Key	RSA	#1805	2048-bit key used during ISAKMP/IKEv2 authentication.
Hashing	SHS	#2896, #2897, #2898	SHA-1 (disallowed for signature generation), SHA-224, SHA-256, SHA-384, SHA-512. Used during ESP.
Message Authentication Code	HMAC	#2244	HMAC-SHA-256 is used for integrity checking the module.
Random number generator	HASH DRBG and Entropy source	#877	Symmetric key generation seeded by /dev/urandom
Key Management	IKE KDF	#587	

Figure 5 Approved Algorithms

For each approved Key Derivation Function the module supports or uses a corresponding protocol. Any such related protocol can be used in the approved mode of operation, but has not been reviewed or tested by the CAVP and CMVP as testing such protocols is not within the scope of CMVP or CAVP activities.

2.2.4.2 Non-approved algorithms allowed in approved mode

- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength).
- Triple-DES (CAVP certificate #1974) key wrapping (key wrapping; key establishment methodology provides 112 bits of encryption strength). Not compliant with the NIST key transport standards (IG D.9).
- The NDRNG that provides the entropy used to seed the random number generator.

2.2.4.3 Non-approved algorithms

When deployed in the Spectre V3 LTE router platform, the router software is configured to only use the cryptographic module in an approved mode of operation. There are no non-approved algorithms available in the FIPS mode of operation.

2.2.5 Components excluded from the security requirements of the standard

There are no components excluded from the security requirements of the standard.

2.3 Physical ports and logical interfaces

The module is classified as a multi-chip standalone module for FIPS 140-2 purposes. The module's physical boundary is that of the device on which it is installed. The device supports sufficient interfaces to allow operators to initiate cryptographic operations and determine the module status.

The module provides its logical interfaces via Application Programming Interface (API) calls. This logical interface exposes services (described in section 2.4.2) that applications utilize directly.

The logical interfaces provided by the module are mapped onto the FIPS 140-2 logical interfaces: data input, data output, control input, and status output as follows:

FIPS 140-2 Logical Interface	Module Mapping
Data Input	Parameters passed to the module via API calls
Data Output	Data returned from the module via API calls
Control Input	API Calls and/or parameters passed to API calls
Status Output	Information received in response to API calls
Power Interface	There is no separate power or maintenance access interface beyond the power interface provided by the device the contains the module

Figure 6 Module Interfaces

2.4 Roles, Services and Authentication

2.4.1 Roles

The Cryptographic Module implements both a Crypto Officer role and a User role. Roles are assumed implicitly upon accessing the associated services. Section 2.4.2 summarizes the services available to each role.

ROLE	DESCRIPTION
Crypto Officer	The administrator of the module having full configuration and key management privileges.
User	General User of the module

Figure 7 Roles

2.4.2 Services

Most of the services provided by the module are provided via access to API calls using interfaces exposed by the module.

However, some of the services, such as power-up module integrity testing are performed automatically and so have no function API, but do provide status output. Other services are accessed via a command line interface (CLI).

Full details of the API functions are provided separately or are available online (https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/Reference/NSS_cryptographic_module/FIPS_mode_of_operation for NSS services and, https://www.kernel.org/doc/Documentation/crypto/api-intro.txt for Kernel crypto API and http://linux.die.net/man/8/ipsec_pluto for pluto and whack).

SERVICE	ROLE	API	DESCRIPTION
Module installation:			
Installation	Crypto Officer	None	The module is deployed as part of a Advantech B+B SmartWorx product installation.
Uninstallation	Crypto Officer	None	The module is uninstalled during the uninstallation of the product that deployed the module.
IPsec:			
Manage Pluto IKE Daemon	Crypto Officer	pluto and whack CLI.	Start, stop and configure the IKE daemon.
Negotiate IKE to establish security	User, Crypto Officer		Protocol exchange to establish Security

SERVICE	ROLE	API	DESCRIPTION
associations			Associations between a pair of nodes.
Kernel Crypto API:			
Symmetric encryption and decryption	User, Crypto Officer	crypto_alloc_blkcipher crypto_blkcipher_encrypt crypto_blkcipher_decrypt crypto_blkcipher_setkey crypto_blkcipher_ivsize crypto_blkcipher_set_iv crypto_free_blkcipher	AES and three-key Triple DES. ECB, CBC and CTR (AES-only) in approved mode.
SHS	User, Crypto Officer	crypto_alloc_hash crypto_hash_setkey crypto_hash_digest crypto_hash_init crypto_hash_update crypto_hash_final crypto_free_hash	SHA-224, SHA-256, SHA-384, SHA-512 in approved mode, SHA-1 may be used in approved mode for non-digital signature generation applications. SHA-1 non-approved for digital signature applications.
NSS:			
PKCS #11	Crypto Officer	FC_GetFunctionList	Returns the list of function pointers to the PKCS #11 functions available in the FIPS Approved mode of operation.
Approved Functions	Crypto Officer	FREEBL_GetVector	Returns a table of function pointers that can be used to access the functions available in the FIPS Approved mode of operation.
Other required services:			
Show Status	User	Status request	Module status. Status is returned in response to individual service API calls; and/or LED indicators; and at the completion of the self-tests.

Service	Role	Api	Description
Self-tests	User	None	Self-tests run automatically at power up. Includes KATs for all approved algorithms and HMAC-SHA-512 for integrity testing of the cryptographic module.
Key zeroization	Crypto Officer	Zeroization request	Zeros (actively overwrites) all plaintext secret, plaintext private keys and other plaintext CSPs.

Figure 8 Services

Notes:

SHA-1 for non-digital signature applications:
SHA-1 is not allowed for digital signature generation. For all other hash function applications, the use of SHA-1 is acceptable. The other applications include HMAC, Key Derivation Functions (KDFs), Random Number Generation (RNGs and RBGs), and hash-only applications (e.g., hashing passwords and using SHA-1 to compute a checksum, such as the approved integrity technique specified in Section 4.6.1 of [FIPS 140-2]).

2.4.3 Authentication

The module has been evaluated at FIPS 140-2 level 1 and no claims are made for authentication.

2.5 Physical Security

The Cryptographic Module is a software-only cryptographic module and therefore the physical security requirements of FIPS 140-2 do not apply.

2.6 Operational Environment

Advantech B+B SmartWorx's proprietary Conel embedded Linux version 5 provides a modifiable operational environment.

The Cryptographic Module is characterized as a software module.

2.7 Cryptographic Key Management

2.7.1 Random Number Generators

The module contains an approved HMAC-SHA-256 SP 800-90A approved DRBG. Checks are made to ensure that the quality of the entropy remains high enough to be used to seed the DRBG.

The module gets entropy from the Linux kernel /dev/urandom library. This entropy seeds the DRBG. Entropy is collected from user key presses and timer information from user input and network events. The seed input to the DRBG is obtained by a call to dev/urandom requesting a minimum of 440 bits of entropy.

The NDRNG is outside of the logical boundary, but within the physical boundary. It produces a minimum of 437 bits of entropy per each GET request.

2.7.2 Key Generation

The module generates keys using an approved key generation mechanism made up of an SP 800-90A HASH_DRBG and available entropy conditioned by /dev/urandom.

2.7.3 Key Table

The following tables list all of the keys and CSPs within the module, describe their purpose, and describe how each key is generated, entered and output, stored and destroyed.

KEY	PURPOSE
CA Public Key	To secure user certificates.
User Public Key	To encrypt data or keys or verify a signature using one of the asymmetric encryption services. Used during OpenVPN (TLS) and IPsec (IKE) key exchange.
User Private Key	To decrypt data or keys previously encrypted by the Public Key or to generate a signature. Used during OpenVPN (TLS) and IPsec (IKE) key exchange.
Peer Public Key	To encrypt data or key material to be sent to a peer module or to verify a signature created by a peer module. Used during OpenVPN (TLS) and IPsec (IKE) key exchange.
HMAC Software Integrity CSP	Used during software integrity test.
ISAKMP Key	ISAKMP Security Association tunnel encryption key
IKE Key	IKE Security Association tunnel encryption key.
IPSEC Key	IPSEC Security Association tunnel encryption keys (one transmit key and one receive key per node)
Diffie-Hellman parameters	Diffie-Hellman key exchange is used to establish the keys used to secure the Security Associations.
DRBG SP 800-90A HASH_DRBG seed input	Random-bit generator
DRBG SP 800-90A HASH_DRBG V & C values	Random-bit generator

Figure 9 Module Cryptographic Keys and CSPs

Note: "Service" keys. A number of the service APIs are for functions that perform cryptographic operations. Some of these accept keys as parameters. There are also APIs for functions that generate keys and pass them back to the calling application. These keys are ephemeral. They are not stored within the module. After these keys have been used by the API functions, they are zeroized within the module. It is the responsibility of the calling application to ensure that it stores, handles and destroys keys appropriately.

Key	Key length/Strength	Generation/Establishment	Storage Location
CA Public Key	RSA 2048-bit	Externally generated	RAM
User Public Key	RSA 2048-bit	Externally generated	RAM
User Private Key	RSA 2048-bit	Externally generated	RAM
Peer Public Key	RSA 2048-bit	Externally generated	RAM
HMAC Software Integrity CSP	512-bit HMAC key	Externally generated	RAM
ISAKMP Key	Diffie-Hellman 2048-bit key	Internally generated	RAM
IKE Key	AES 256-bit or Triple DES 192-bit	Internally generated	RAM
IPSEC Key	AES 256-bit or Triple DES 192-bit	Internally generated	RAM
Diffie-Hellman parameters	AES 256-bit or Triple DES 192-bit	Internally generated	RAM
DRBG SP 800-90A HASH_DRBG seed input	Seed input of 440 bits according to SP 800-90A.	Generated by gathering entropy	RAM
DRBG SP 800-90A HASH_DRBG V & C values	Internal state for the Hash_DRBG	Internal state derived from seed value	RAM

Figure 10 Key Table part 1

KEY	ARE KEYS STORED ENCRYPTED OR PLAINTEXT?	ENTRY/OUTPUT	DESTRUCTION
CA Public Key	Plaintext	N/A	Zeroized using the key zeroization service.
User Public Key	Plaintext	N/A	Zeroized using the key zeroization service.
User Private Key	Plaintext	N/A	Zeroized using the key zeroization service.
Peer Public Key	Plaintext	N/A	Zeroized using the key zeroization service.
HMAC Software Integrity CSP	Plaintext	N/A	Zeroized using the key zeroization service.
ISAKMP Key	N/A	N/A	Zeroized using the key zeroization service.
IKE Key	N/A	N/A	Zeroized using the key zeroization service.
IPSEC Key	N/A	N/A	Zeroized using the key zeroization service.
Diffie-Hellman parameters	N/A	N/A	Zeroized using the key zeroization service.
DRBG SP 800-90A HASH_DRBG seed input	N/A	N/A	Zeroized using the key zeroization service.
DRBG SP 800-90A HASH_DRBG V & C values	N/A	N/A	Zeroized using the key zeroization service.

Figure 11 Key Table part 2

2.7.4 Key Destruction

All key material managed by the module can be zeroized using the key zeroization service.

In this way all key material and CSPs are zeroized. There are no user-accessible plaintext keys or CSPs in the module.

2.7.5 Access to Key Material

The following table shows the access that an operator has to specific keys or other critical security parameters when performing each of the services relevant to his/her role.

KEY												
Services	**Role**	**CA PUBLIC KEY**	**USER PUBLIC KEY**	**USER PRIVATE KEY**	**PEER PUBLIC KEY**	**ISAKMP KEY**	**HMAC S/W INTEGRITY CSP**	**IKE KEY**	**IPSEC KEY**	**DIFFIE-HELLMAN PARAMETERS**	**HASH_DRBG SEED INPUT**	**HASH_DRBG V&C**
Installation	CO											
Uninstallation	CO											
Manage Pluto IKE Daemon	CO	W	W	W								
Negotiate IKE to establish Security Associations	CO, User				W	W		W	W	W	U	U
Symmetric encryption and decryption	CO, User					U		U	U			
SHS	CO, User											
PKCS #11	CO											
Approved functions	CO										U	U
Show Status	User											
Self-tests	User						U					
Key zeroization	CO	W	W	W	W	W		W	W	W	W	W

Figure 12 Access to keys by services

Access Rights	Blank	N/A
	R	Read
	W	Write
	U	Use

Note: Key zeroization zeroes all keys and CSPs, this is a “write” operation in that all keys are overwritten with zeroes.

2.8 Self-Tests

The module implements both power-up and conditional self-tests as required by FIPS 140-2. The following two sections outline the tests that are performed.

2.8.1 Power-up self-tests

The following table lists the power-up self-tests performed by the module. The module contains several distinct implementations of each approved algorithm and performs a distinct power-up self-test for each implementation.

For clarity, the table identifies each approved algorithm, the test performed, and the CAVP certificate number for each implementation.

OBJECT	TEST	IMPLEMENTATION (CAVP CERT #)
SHS	Known answer test (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)	#2896, #2897, #2898
AES-256 Encrypt	Known answer test	#3515, #3516
Triple DES Encrypt	Known answer test	#1974, #1975
AES-256 Decrypt	Known answer test	#3515, #3516
Triple DES Decrypt	Known answer test	#1974, #1975
HMAC	Known answer test (HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512)	#2244
HMAC DRBG	Known answer test	#877
RSA	Known answer test	#1805
Module software	HMAC-SHA-256 integrity check	#2244

Figure 13 Power-up self-tests

2.8.2 Conditional self-tests

EVENT	TEST	CONSEQUENCE OF FAILURE
Module requests a random number from the FIPS Approved SP800-90 DRBG	A continuous random number generator test	Random number is not generated and module enters an error state.

Figure 14 Conditional self-tests

Note: The module seeds the DRBG once at startup using a call to dev/urandom. This PRNG is outside the scope of the logical boundary of the module and the module does not apply a CRNG test to it.

2.9 Design Assurance

Advantech B+B SmartWorx employ industry standard best practices in the design, development, production and maintenance of all of its products, including the FIPS 140-2 module.

This includes the use of an industry standard configuration management system that is operated in accordance with the requirements of FIPS 140-2, such that each configuration item that forms part of the module is stored with a label corresponding to the version of the module and that the module and all of its associated documentation can be regenerated from the configuration management system with reference to the relevant version number.

Design documentation for the module is maintained to provide clear and consistent information within the document hierarchy to enable transparent traceability between corresponding areas throughout the document hierarchy, for instance, between elements of this Cryptographic Module Security Policy (CMSP) and the design documentation.

Guidance appropriate to an operator's Role is provided with the module and provides all of the necessary assistance to enable the secure operation of the module by an operator, including the Approved security functions of the module.

Delivery of the Cryptographic Module to customers from the vendor is via secure courier. The cryptographic module is pre-installed in a router device in the vendor manufacturing facility.

2.10 Mitigation of Other Attacks

The module does not mitigate any other attacks.

3 Secure Operation

The module is deployed pre-installed and configured to operate in a FIPS mode of operation as an integral part of a Advantech B+B SmartWorx router. No User or Crypto Officer actions are required to ensure that the module is capable of operating in a FIPS 140-2 compliant mode of operation.

The evaluated module was tested on the Spectre V3 LTE router.

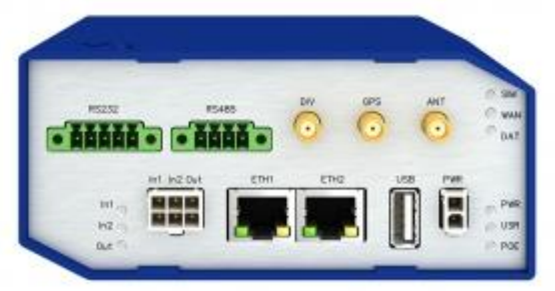

Figure 15 Spectre V3 LTE Router

If an operator wants to operate with non-FIPS 140-2 software, the Crypto Officer must uninstall the deployed software image and install a new one. This will render the router non-FIPS compliant and is not recommended in environments where FIPS 140-2 is required.